DENISE M. MINGRONE (STATE BAR NO. 135224)
dmingrone@orrick.com
ROBERT L. URIARTE (STATE BAR NO. 258274)
ruriarte@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025-1015
Telephone: +1 650 614 7400
Facsimile: +1 650 614 7401

CLAUDIA WILSON FROST (*Pro Hac Vice*)
cfrost@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
609 Main Street, 40th Floor
Houston, TX 77002-3106
Telephone: +1 713 658 6460
Facsimile: +1 713 658 6401

Attorneys for Plaintiff
SYNOPSYS, INC.

IN THE UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

SYNOPSYS, INC., Plaintiff, v. UBIQUITI NETWORKS, INC., UBIQUITI NETWORKS INTERNATIONAL LIMITED, CHING-HAN TSAI, and DOES 1-20, inclusive, Defendants.	Case No. 3:17-cv-00561-WHO **SYNOPSYS, INC.'S MOTION FOR SANCTIONS FOR SPOLIATION** **[REDACTED PUBLIC VERSION]** Date: November 7, 2018 Time: 2:00 p.m. Dept: Courtroom 2, 17th Floor Judge: Hon. William H. Orrick
UBIQUITI NETWORKS, INC. AND UBIQUITI NETWORKS INTERNATIONAL LIMITED, Counterclaimants, v. SYNOPSYS, INC., Counterdefendant.	

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

NOTICE OF MOTION AND MOTION

TO ALL PARTIES AND THEIR COUNSEL OF RECORD: PLEASE TAKE NOTICE that the following Motion for Sanctions for Spoliation will be heard on November 7, 2018 at 2:00 p.m., or as soon thereafter as counsel may be heard, in Courtroom 2, 17th Floor of this Court located at 450 Golden Gate Avenue, San Francisco, California, the Honorable William H. Orrick presiding. Plaintiff Synopsys, Inc. ("Synopsys") hereby moves for sanctions under the Court's inherent powers and Federal Rule of Civil Procedure 37 against Defendants Ubiquiti Networks, Inc. ("Ubiquiti"), Ubiquiti Networks International Limited ("UNIL"), and Ching-Han Tsai (collectively, "Defendants") for deliberate and widespread spoliation of evidence. Defendants' pervasive and permanent destruction of evidence has hampered Synopsys' ability to prove its Digital Millennium Copyright Act ("DMCA") claims, including the nature, number, and circumstances of Defendants' circumventions of Synopsys' security measures and Defendants' manufacture, provision, and trafficking of circumvention technology, products, services, and devices. In light of Defendants' willful and egregious spoliation, Synopsys seeks a sanction of default judgment against all Defendants on the First, Second, and Third Claims for Relief, for violations of the DMCA, 17 U.S.C. §§ 1201(a)(1), (a)(2), and (b), respectively. Specifically, Synopsys requests that this Court accept as established the allegations in the Third Amended Complaint and enter a default judgment that Defendants are liable for 38,393 violations of the DMCA, with damages for those violations to be determined at a later date.

In the alternative, if the Court declines to grant default judgment, the Court should issue all, or at the very least some combination of, the following: (1) an order precluding Defendants from contesting the number of circumventions, as shown in the call-home data, (2) an order precluding Defendants from contesting that the circumventions and traffickings are violations of the DMCA, compensable under the law, and are not extraterritorial, (3) an instruction (the precise language of which will be determined at a later date) that the jury shall infer that the destroyed evidence was incriminating in that it tended to prove Defendants' violations of the DMCA, including, but not limited to, that Defendants' violations "occurred in the United States," *see RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2101 (2016), and (4) any and all other relief as this Court deems appropriate. In the event alternative relief is ordered, Synopsys should have the full right to prove the extent of spoliation to the jury.

This Motion is based on this Notice of Motion and Motion, the following Memorandum of Points and Authorities, the declarations and the material attached thereto, the record in this matter, and any other and further papers, evidence, and argument as may be submitted in connection with this Motion.

I. INTRODUCTION

This lawsuit arises out of Defendants' elaborate scheme to pirate Synopsys' EDA software, through the use of counterfeit license keys and fraud, so that Defendants Ubiquiti and UNIL could design a semiconductor chip without paying millions of dollars in licensing fees. Forensic examination of Defendants' computers, servers, and other devices proves that virtually all the members of Ubiquiti's chip design team—no less than eight Ubiquiti and UNIL employees—destroyed evidence after Ubiquiti and UNIL were put on notice of Synopsys' claims and even after Synopsys filed suit. The deleted evidence includes logs recording the number of unauthorized uses of Synopsys' software, incriminating communications among piracy team members, counterfeit license keys used to illegally access Synopsys' software, executable code for the pirated software, and virtual machines on which the pirated software was used.

The scope of the spoliation is enormous and largely undisputed by Defendants (though they quibble with how much evidence was destroyed and precisely when). For example,

- Defendant Ching-Han Tsai, the manager of the design team that executed the piracy, deleted tens of thousands of files from the "Synopsys" folder on his computers linked to a cloud storage account (which itself was never produced).
- Tsai deleted from his hard drive a virtual machine he used to illegally run Synopsys software over one thousand times as well as the virtual machine's command history log ("bash history") which would have logged additional executions of which Synopsys is not aware.
- A number of members of the design team, including Josh Huang, Chang-Ching Yang, and Ya-Chau Yang, used computer wiping tools, such as CCleaner, AVG "File Shredder," and "IOBit Advanced System Care," to permanently delete key evidence from their computers.
- James Lian not only deleted critical evidence from his external hard drive, such as logs of Synopsys software usage and counterfeit keys, he searched for the term "Synopsys" and edited locations known to contain references to Synopsys software on his devices.
- The spoliators also deleted from the UNIL servers the virtual machines used to carry out the piracy, counterfeit keys and counterfeit key generating software, and the logs that recorded the unlicensed usage of Synopsys' software.

Defendants' spoliation was executed to frustrate not only Synopsys' ability to prove its claims, but the Court's orders. Many of the deletions occurred after Synopsys brought suit in February 2017 and in February and March 2018, after Judge Beeler overruled Defendants' attempts to prevent discovery of many of the design team's devices. Deletions often occurred just days, hours, or even minutes before the devices were collected for inspection and production:

- Huang ran CCleaner two times the day his computer was imaged, including just *37 minutes* before imaging. Ubiquiti's VP of Legal Affairs, in justifying Huang's termination for destroying evidence, put "[t]he likelihood of th[at] being a coincidence [at] exactly 0%." Ex. A.[1]
- C.C. Yang downloaded and ran CCleaner the day before his computer was scheduled for imaging, deleting almost 5,000 files and 20 folders.
- Y.C. Yang used two different shredding programs long after this litigation began, including twice in February 2018, after Judge Beeler's discovery order.
- Tsai ran CCleaner to permanently delete specific files, folders, and evidence of other deletions on his external hard drive the day before it was imaged.

Ubiquiti management not only failed to prevent the spoliation but facilitated it by abdicating any meaningful oversight or responsibility for preserving evidence. After being put on notice that its employees were pirating Synopsys' software, Ubiquiti failed to take steps to ensure that evidence was preserved, such as imaging, inspecting, or quarantining team member devices. Ubiquiti gave Tsai sole responsibility for collecting evidence of his team's misconduct, even though Tsai's role as manager of that team and his own conduct implicated him in the piracy. Unsurprisingly, instead of collecting evidence, Tsai led the effort to destroy it—and then pleaded the Fifth Amendment when asked whether he destroyed evidence. Finally, Defendants' dilatory discovery tactics successfully forestalled forensic review of the devices, leaving Tsai and his team ample time to complete the spoliation and causing untold amounts of data on crucial servers to be deleted through automatic deletion settings Defendants never suspended during litigation.

The prejudice to Synopsys cannot be overstated. Were it not for Defendants' widespread and willful spoliation, this case would be all but over: Incriminating information on Defendants'

[1] All Exhibit references are to the Declaration of Denise M. Mingrone, unless otherwise stated.

devices would have foreclosed their defenses, and Synopsys would have complete information on the who, what, where, when, and how of Defendants' illegality. Instead, Synopsys, the Court, and the jury will never know the full extent of Defendants' misconduct. Even worse, Defendants intend to profit from their spoliation by assailing the accuracy of the "call-home" data generated by Synopsys' software and by claiming that their activities occurred outside the United States, even though Defendants destroyed evidence corroborating the call-home data and their spoliation has impeded Synopsys' ability to prove Defendants' illegal activities were not extraterritorial.

Defendants' conduct therefore warrants a terminating sanction as to Synopsys' DMCA claims. Synopsys requests default judgment against all Defendants that Defendants are liable and Synopsys can recover damages **(1)** on Claim 1 for 38,393 circumventions in violation of the DMCA, 17 U.S.C. § 1201(a)(1), as alleged in ¶ 32 of the Third Amended Complaint ("Complaint")[2] and **(2)** on Claims 2 and 3 for 38,393 unlawful acts of manufacturing, providing, or trafficking circumvention technology, products, and services in violation of the DMCA, 17 U.S.C. § 1201(a)(2), (b), as alleged in ¶¶ 69-73, 83-89, 137-38, & 154-56 of the Complaint.

Synopsys does not make this request lightly, but a sanction of default is necessary in light of the magnitude of Defendants' spoliation and the importance of the evidence destroyed. Besides challenging as unreliable Synopsys' call-home data, Defendants argue that the circumventions and traffickings are not compensable violations of the DMCA because they occurred outside the United States and the DMCA does not apply extraterritorially. Even a preclusion sanction order accepting 38,393 circumventions does not protect Synopsys or ensure that Defendants do not benefit from their spoliation by asserting extraterritoriality. Defendants' willful spoliation destroyed critical evidence that Synopsys could have used to rebut Defendants' arguments of no nexus to the United States and that Defendants' relevant conduct occurred abroad. The only way to safeguard Synopsys from the harms of Defendants' spoliation is a default judgment of 38,393 *violations* of the DMCA that are compensable under the law.[3]

[2] The Complaint alleged in round numbers that there were more than 39,000 DMCA violations. Synopsys seeks a sanction of default judgment for 38,393 violations that are reflected in the call-home data. Ex. B.

[3] To preserve its rights, Synopsys alternatively requests specified preclusion orders, adverse inference instructions, and all other relief this Court deems appropriate. *Supra* I-II.

II. FACTUAL BACKGROUND

A. An Overview of the Evidence Destroyed and Its Significance.

Section 1201(a)(1) of the DMCA prohibits circumvention of security measures controlling access to copyrighted software, and § 1201(a)(2) and (b) prohibit trafficking in circumvention technology, devices, and services. Each circumvention and each act of trafficking is a separate violation, for which Synopsys is entitled to actual or statutory damages. 17 U.S.C. § 1203(c).

This case involves circumvention of Synopsys' security measures. Synopsys' EDA software requires a "license key" in order to be run by a user. *See* Ex. C at 107:1-5. Ubiquiti and UNIL circumvented these access controls by using counterfeit license keys. Ex. D (Report of Synopsys Forensic Expert, Daniel Roffman) at 40; Ex. E (Ubiquiti Interrogatory Resp.) at 10; Ex. G (UNIL Interrogatory Resp.) at 10-11; Ex. H (Tsai Interrogatory Resp.) at 11.

[redacted] *See* Ex. C at 146:11-14.[4] [redacted] *See* Ex. C at 147:20-148:14; Ex. D at 21; Ex. I ¶¶ 39-43, 47, 63, 93, 95.

Logs generated by Synopsys tools are in addition to, and can be correlated with, command history logs on the user's computer that are automatically created by Linux operating systems. These command history files, known as "bash history" logs, record all commands executed on the operating system. Roffman Decl. ¶¶ 22-24. Bash history logs would show, for example, the commands used to install a Synopsys application, start a Synopsys license server, or run a Synopsys application. *See id.*

In addition to log information saved locally, the security measures on Synopsys' software also document unauthorized use by generating "call-home" data and transmitting it back to Synopsys. *See* Ex. K at 339:18-22; Ex. I ¶¶ 26, 39-43, 47, 73, 86, 93, 95. [redacted]

[4] [redacted] *Id.* at 147:8-13. [redacted] *Id.* at 15, 24; Ex. J at 245:4-11.

[redacted] *See* Ex. C at 159:12-24; Ex. K at 514:14-24. Each time Synopsys' software is used without authorization, the security software generates an alert to be sent back to Synopsys. *See* Ex. K at 339:9-15. Synopsys received 38,393 call-home alerts over the months of Defendants' illegal use through mid-June 2016, after which Defendants intentionally reconfigured their servers to block further call-home signals from reaching Synopsys. Ex. B; Ex. D (Roffman Report) at 8-9, 45-46. Though there were more unauthorized uses after mid-June 2016, Synopsys seeks default judgment for only the 38,393 reported incidents. Ex. L at 18.[5]

Attempting to limit or avoid liability for the pre-May 2016 uses, [redacted] Ex. M (Defendants' expert) ¶ 25. [redacted] *See* Ex. C at 159:12-24; Ex. K 514:14-24; *see also* Ex. D at 30-31 (comparing recovered log artifacts with call-home data); Ex. J at 97:16-100:1, 101:14-102:1 (same). Bash history logs would similarly have corroborated the call-home data by showing the specific commands executed on each device. Roffman Decl. ¶ 22.

In addition, as mentioned, the local logs would have shown additional incidents of illegal use after Defendants manipulated their firewall to block the transmission of call-home signals back to Synopsys. Ex. N (Tsai-Wang conversation) (after Synopsys notified Ubiquiti that it had received call-home data indicating illegal software use, Tsai and his team "reconfigur[ed] [their] firewall to block all outgoing traffic," including the call-home data). The illegal use of the software continued, Ex. D at 8, 19-23, and the local logs and computer bash history would have proved and quantified it. But, because Defendants blocked the signal back to Synopsys and destroyed the incriminating evidence stored locally, Synopsys has been deprived of key evidence of the number and circumstances of the piracy. Ex. D at 9-10, 45-59.

[5] Synopsys contends that Defendants committed an additional 16,434 circumventions from June 2016 through November 2017 (913 a month for 18 months) for a total of 54,827 violations. Ex. L at 40-41. Synopsys has not sought default for the larger figure, though it would have been entitled to it. If this matter proceeds to trial without a default judgment on Synopsys' DMCA claims, Synopsys reserves the right and intends to recover for the full number of violations.

B. Defendants' Illegal Use of Synopsys' Software.

In 2013, Ubiquiti needed EDA software to design an application-specific integrated circuit ("ASIC") for its upcoming AirMax Evolution line of products, which Ubiquiti was counting on to be "a really big differentiator in the market." Ex. O at 78. Ubiquiti hired Tsai to lead the "AME Project," to report directly to the CEO, and to recruit and manage the design team (the "AME team") and procure EDA software. From the outset of the project, Tsai was aware: "If we can use piracy, then we can save some money." Ex. P at 86 (line 3782) (Y.C. Yang speaking to Tsai).

In September 2013, Tsai contacted Synopsys on behalf of Ubiquiti and requested information on various Synopsys tools. *See* Ex. Q at 40:18-41:22, 114:8-16. In late 2013, based on Tsai's misrepresentations that Ubiquiti and UNIL were sincerely interested in licensing Synopsys' software, Synopsys granted Ubiquiti an evaluation license,[6] and Ubiquiti/UNIL downloaded Synopsys' software and documentation. *See* Ex. G (UNIL Interrogatory Resp.) at 13. After the evaluation period ended, however, Defendants did not purchase a license to Synopsys' software. Instead, they carried out their plan to use Synopsys' software without paying for it by illegally creating or obtaining counterfeit license keys.

Defendants do not dispute that Tsai and the AME team pirated Synopsys' software. *See* Ex. OO (Ubiquiti & UNIL Opp. to Synopsys Mot. to Amend) at 2-3 ("Tsai informed Ubiquiti management that he had investigated further and determined that some engineers on the ASIC project had used Synopsys software without a license[.]"); Ex. PP (Nisenbaum Decl.) ¶ 6 (Ubiquiti Executive VP of Legal Affairs) (Ubiquiti came to "learn[] that Defendant Tsai had lied to Ubiquiti management regarding the use of Synopsys software in Taiwan (including his own use of the software)."). [redacted] Ex. M (Defendants' expert) ¶ 25. Defendants dispute the 38,393 figure from the call-home data and whether they are domestic violations of the DMCA compensable under the law.

C. Defendants' Systematic, Pervasive, and Deliberate Spoliation.

[redacted]

[6] An evaluation license is a short-term license to try software. The evaluation license here was 90 days starting November 26, 2013 and expressly limited the use of Synopsys software. Ex. R.

[redacted] Ex. S. [redacted] *Id.* at 80. [redacted] *Id.*

[redacted] *See, e.g.*, Ex. T. [redacted] Ex. U at 50, [redacted] Ex. T at 70-71. [redacted] *Supra* 5.

The parties were unable to reach a resolution, and Synopsys filed this action on February 3, 2017. On May 12, 2017, Synopsys served its first set of requests for production seeking, *inter alia*, "All COMPUTERS used by [Ubiquiti and UNIL] containing copies of Synopsys SOFTWARE, DOCUMENTATION, or LICENSE KEYS during the time period from January 1, 2013 to present." Exs. V (Ubiquiti) No. 35; W (UNIL) No. 35. On September 8, 2017, Synopsys served additional targeted requests to inspect and image specified servers and computers (identified by MAC address, username, and IP address). Exs. X (Ubiquiti); Y (UNIL).

Defendants' dilatory tactics significantly delayed production of this information for nearly a year after the complaint was filed. *See* Ex. F (discovery timeline). It appears Defendants' "foot-dragging," Ex. WW (J. Beeler Order) at 2, created the opportunity for the AME Team to destroy evidence on a massive scale. When Synopsys was finally granted access to review and inspect Defendants' devices in March 2018, Synopsys learned that the AME Team's data had not been preserved and that the AME Team had permanently deleted thousands of relevant files, both after the ITCA Notice and after Synopsys filed this suit. Ex. D (Roffman Report) at 48-59.

Defendants concede that spoliation has occurred. *See, e.g.*, Ex. QQ (Ubiquiti & UNIL Answer) ¶ 121 ("Ubiquiti Defendants admit that Defendant Tsai used a software program called CCleaner on an external drive[.]"); Ex. PP (Nisenbaum Decl.) ¶ 4 (same). [redacted] *See* Exs. A, Z-CC (Termination Notices). Defendants instead claim that they do not know the contents of the deleted files—which, of course, is precisely why litigants are required to preserve evidence in the first place.

A full accounting of Defendants' known spoliation is set forth in the report of forensics expert Daniel Roffman (Ex. D at 9-10, 45-59). Below are some of the most egregious instances of spoliation uncovered during discovery. *See* Roffman Decl. (filed contemporaneously).

Tsai's Devices. Synopsys' forensic analysis discovered substantial deletions across a host of Tsai's devices, forming a "pattern[] of deletions," which often occurred in "close proximity" to when Synopsys filed its complaint or when Tsai's devices were supposed to be imaged or inspected. Ex. D at 53; Roffman Decl. ¶¶ 7.vii.-ix.

[redacted] *Id.* at 9. [redacted] *Id.* at 53. [redacted] *Id.* [redacted] Ex. DD at 179:3-11.

On November 16, 2017, *the day prior to imaging*, Tsai used CCleaner wiping software to "permanently" delete "specific files, folders, and the unallocated space on the [external] hard drive." Ex. D at 56; Roffman Decl. ¶ 7.viii. CCleaner permanently removes data; it is advertised as a method to "thwart most attempts at recovery." Ex. MM. Wiping the unallocated space on a hard drive is particularly telling because that is where remnants of deleted data remain until overwritten. Ex. D at 20. All told, Tsai used CCleaner to "permanently" delete and overwrite approximately 248,000 files. *Id.* at 10, 56. Ubiquiti and UNIL admit that Tsai used CCleaner. Ex. QQ (Ubiquiti & UNIL Answer) ¶ 121. Tsai also loaned a USB drive with a "portable copy of … CCleaner" to at least two other AME Team members. Roffman Decl. ¶ 7.viii.

In addition, Tsai deleted some virtual machines and the data from other virtual machines, including one with the host name "AME-VM1." *Id.* ¶ 13. AME-VM1 was one of the host names in Synopsys' call-home data, and thus its data would have provided evidence to corroborate Synopsys' call-home data. *Id.* [redacted] Roffman Decl. ¶ 7.ix.; Ex. D at 10, 29; *cf. id.* at 33 [redacted]

On November 16, 2017, Tsai deleted the contents of the bash history data for the virtual machine, which contained a log of commands executed, such as those related to use of Synopsys' software. Roffman Decl. ¶ 23. The only remaining commands in the bash history after November 16, 2017 related to viewing the contents of the bash history, deleting it, and then viewing it again—"presumably to confirm it was deleted." Ex. D at 52. [redacted] Ex. DD at 63:8-64:3.

Examination of Tsai's Ubiquiti devices uncovered several other devices that had never been preserved and produced, including an additional laptop, an additional internal hard drive from one of his laptops, two USB drives, and several cloud storage accounts. Ex. D at 47, 42; Roffman Decl. ¶ 27. During his deposition on April 15, 2018, Tsai acknowledged the existence of the additional laptop, which he used for Ubiquiti work purposes, but which had not been collected or inspected. *See* Ex. DD at 315:13-318:18. Several days later, Synopsys received a forensic image of that laptop, but, by then, relevant information had been destroyed. Ex. D at 53. Indeed, on December 11, 2017, Tsai "'soft deleted'" off that laptop (*i.e.*, sent to the recycle bin) 30,724 files from a Synopsys folder linked to his OneDrive account. *Id.*; *see* Roffman Decl. ¶ 7.vii. Tsai also ran CCleaner on the laptop's hard drive on November 16, 2017. *Id.* ¶ 7.viii.

Other Members of the AME Team. Tsai was not the only member of the AME Team busy destroying evidence. Nearly every key custodian took similar actions, in some instances only days—or even minutes—before their devices were inspected.

<u>Josh Huang</u>: Huang ran CCleaner twice on March 12, 2018—more than a year after Synopsys filed its complaint—just *37 minutes* before his laptop was imaged. Roffman Decl. ¶ 7.xii. [redacted] Ex. A at 41. Artifacts in the unallocated space on his computer indicate that Huang previously possessed, and had since deleted, "counterfeit licenses or license key generators" for Synopsys applications, Ex. D at 54, as well as "cracked" Synopsys applications, *i.e.*, applications that have "been manipulated to remove or disable features such as licensing restrictions or advertisements," Roffman Decl. ¶ 7.

<u>Ya-Chau Yang</u>: Y.C. Yang used two shredding programs—AVG File Shredder and IObit Advanced SystemCare—to permanently delete 64 folders and 134 files on his laptop on February 8, 2018.[7] Roffman Decl. ¶ 7.xvi. Yang also used those shredding programs on September 27, 2017, January 24 and 31, 2018, and February 9 and 12, 2018. *Id.*; Ex. D at 57.

On February 9, 2018, Yang deleted a virtual machine, making it "no longer recoverable." Roffman Decl. ¶ 7.xvi. Yang also used IObit Advanced SystemCare to permanently "delete[] [the] internet history data" on his laptop. *Id.*; Ex. D at 57. [redacted] Ex. D at 44; *see id.* at 63 [redacted]

[7] The AVG File Shredder is advertised as "an easy way to permanently and securely delete a file, folder or the *Recycle Bin* contents," such that those deleted items "cannot be recovered even with the use of advanced disk utilities." Ex. NN.

[redacted]

Sheng-Feng (Woody) Wang: W. Wang used yet a different technique to destroy evidence: He copied eight mp4 video files of episodes of "Hunger Games: Taichung City" onto his external hard drive *463 times* in one day—January 27, 2018, three days before the drive was imaged. Roffman Decl. ¶ 7.x.; Ex. D at 10, 57. Because "deleted data sits in unallocated space on a hard drive until it is overwritten," W. Wang's repetitive copying had "the effect of destroying remnants of deleted files." *Id.* at 57. [redacted] Ex. EE at 198:18-199:8. As a result of Wang's overwriting scheme, no Synopsys software could be recovered from his external hard drive. [redacted] Ex. D at 29.

Andre Lee: [redacted] Roffman Decl. ¶ 7.xiii. [redacted] Ex. D at 11.

James Lian: On November 13, 2017, before Lian's devices were imaged, he deleted "Synopsys license keys, logs, and other relevant files," including "a counterfeit license key for Synopsys software," from his external hard drive. Roffman Decl. ¶ 7.xi.; Ex. D at 10, 53-54. Specifically, a virtual machine found on Lian's external hard drive "showed evidence of destruction of log files" as well as evidence that Lian "search[ed] for the term 'Synopsys' and edit[ed] locations known to contain references to Synopsys software."[8] Roffman Decl. ¶ 7.xi. Lian also "zeroed out" the unallocated space on his laptop prior to imaging—*i.e.*, he "overwrote deleted files on the hard drive with zeros." *Id.*

[8] The evidence suggests that some of the deletion on Lian's external hard drive occurred on or after December 8, 2017, in the week prior to the imaging of his devices. *Id.* at 53.

[redacted] Ex. D at 35-36, 38-39. [redacted] *Id.* at 40-41.

[redacted] *Id.* at 55. [redacted] *Id.* [redacted] *Id.* at 48. [redacted] Ex. D at 48. [redacted] *Id.*

Chang-Ching Yang: C.C. Yang's computer was scheduled for imaging on March 14, 2018. The day before, he downloaded and ran CCleaner, permanently deleting almost 5,000 files and 20 folders, as well as system artifacts regarding activities on his computer, which would have explained Yang's USB activity. Roffman Decl. ¶ 7.xiv. C.C. Yang also used IOBit Uninstaller to remove OneDrive software, which prevented forensic search for Synopsys-related data. *Id.*

Hua-Lin Hsu: Hsu's desktop computer contained evidence that Hsu deleted archives of chat communications between him and Tsai discussing how to block Synopsys call-home data. *Id.* ¶ 7.xv; Ex. D at 11, 59. Those chats occurred days after Defendants received the ITCA Notice in May 2016. Hsu deleted those chat logs on February 8, 2018, more than a year after Synopsys filed this suit and shortly before Hsu's drives were imaged on March 12, 2018. *Id.*

[9] UNIL's forensic expert could not locate this virtual machine either. Ex. FF at 7.

In sum, much of the destruction of evidence by the AME Team detailed above occurred in February and March 2018 before their devices were imaged. Roffman Decl. ¶ 7; Ex. D at 56-59. Not only was that more than a year after Synopsys filed its complaint, it was *after* Judge Beeler rejected Defendants' bid to avoid producing those devices. *See* Ex. RR (Jan. 29, 2018 Order). Once Defendants failed in their efforts to prevent production of those devices, the AME Team went to great lengths to delete, wipe, shred, and overwrite their devices to keep Synopsys from discovering the full scope and details of Defendants' piracy.

Defendants' servers. Besides the devices of the AME Team members, the UNIL Taiwan server array was one of the most critical sources of evidence. Indeed, *according to Defendants*, the servers were the primary system used to host and execute Synopsys software. Ex. SS (Defs.' Opp. to Synopsys' Request for Inspection) at 4 (citing Ex. TT (Tsai Decl.)).

When Synopsys' forensic team was finally permitted to inspect the servers on March 16, 2018, more than a year after the complaint was filed, it found significant evidence "suggesting that someone attempted to remove evidence of usage of Synopsys' software." Ex. D at 48. Forensic analysis revealed that "James Lian accessed … Synopsys key generators on UNIL's server," including after Synopsys filed suit, but those files "have since been deleted." *Id.* at 10; *see id.* at 1-21, 39. Forensic analysis also showed that [redacted] *Id.* at 48, 9; *see id.* at 49 [redacted] The very existence of remnants of that data "confirms that Defendants used th[ese] server[s] to infringe and run Synopsys' software," though Defendants' spoliation means the nature, number, place, and time of the unauthorized accesses can no longer be determined. *Id.* at 48.

Perhaps most importantly, the servers once contained the logs created by Synopsys' software which would have showed the amount and circumstances of Defendants' piracy. *Id.* at 19; Roffman Decl. ¶ 7.vi. Someone using the highest privileged credentials entered commands to "delete the bash history" on the AME-W2 server—*i.e.*, the server's "log of past commands," including "past commands used to execute Synopsys software." Ex. D at 19. In addition, someone "executed a command to delete a Synopsys installer folder on [the] AME-W1 [server]," which "would have contained installation logs showing when Synopsys software was installed." Roffman Decl. ¶ 7.vi. "[D]espite [Defendants'] efforts to conceal their activity and destroy evidence," the servers still contain some artifacts of "portions of deleted logs." Ex. D at 19. Those fragments show some of Defendants' use of Synopsys software, including "that Defendants continued using Synopsys' software after Synopsys filed [this] lawsuit." *Id.*

D. Ubiquiti and UNIL Executives Facilitated the Massive Spoliation.

Defendants' destruction of evidence was part of an extensive, organized scheme that was, at the very least, facilitated by Ubiquiti and UNIL executives' failure to enforce their own policies against spoliation and to diligently investigate Synopsys' allegations.

[redacted] Ex. GG (Nisenbaum Dep. Tr.) at 147:11-148:15, 148:25-149:15, 151:15-24, 158:14-21. [redacted] *Id.* at 102:16-19, 103:20-104:7. [redacted] *Id.* at 153:18-24, 154:20-155:16, 166:16-21, 280:10-281:4.

[redacted] *Id.* at 122:23-123:4; *see also* Ex. HH at 518:22-519:1. [redacted] Ex. GG at 166:1-6, 186:9-187:7.

Unsurprisingly, Tsai did not order his team to stop its piracy or to preserve evidence. [redacted]

[redacted] Ex. N. [redacted] Ex. II. The AME team spent more than 140 hours disabling the call-home signals. Ex. TT (Tsai Decl.) ¶ 17.

E. Significant Evidence Was Spoliated While Defendants Resisted Discovery.

A year into the case, Judge Beeler rightly excoriated Defendants' discovery tactics when she instructed them that "[t]his foot-dragging must stop." Ex. WW at 2; *see* Ex. F (discovery timeline). Although Synopsys filed its complaint in February 2017 and requested discovery in May 2017, it was not until November 2017 that Defendants agreed to produce images of any of the requested devices. Even then, Defendants only agreed to produce Tsai's work computers. Ex. UU (Synopsys Mot. for Leave to Amend Compl.) at 4; Ex. VV (Joint Letter) at 4-5 & n.2 (Synopsys footnote, Defendants' text). None of the devices discussed above was imaged, quarantined, or otherwise preserved as of November 2017, which is how members of the AME Team were able to permanently destroy so much evidence before their devices were imaged.

Once Defendants examined the first set of Tsai devices, they quickly realized that there had been spoliation. *See* Ex. PP (Nisenbaum Decl.) ¶ 4 ("During a forensic inspection of [Tsai's] devices in *December 2017*, Ubiquiti discovered that Defendant Tsai had used … CCleaner to wipe portions of his external drive[.]" (emphasis added)). But rather than immediately notify Synopsys and the Court, Ubiquiti and UNIL instead reneged on their agreement to produce Tsai's devices in December 2017 and then delayed producing them until March 2018. Ex. WW (Order) at 2 (Tsai devices not produced by late February).

Perhaps most significantly, Defendants' failure to take any steps to collect and preserve evidence on the UNIL servers, coupled with Defendants' delay in permitting inspection of those servers, resulted in the destruction of critical log files that Defendants *knew* would be automatically deleted or overwritten due to the passage of time. Defendants successfully delayed the server inspection *for months* by raising meritless objections that required multiple rounds of briefing and hearings. *See* ECF Nos. 99, 105, 109, 110, 111, 114, 117, 118, 119, 123, 127, 130, 136; *see also* Ex. F (discovery timeline). Defendants, however, "made no changes to the configurations" of the servers to cancel automatic deletions during the litigation. Ex. JJ at 196:6-24. As a result, every day of Defendants' delay resulted in more and more evidence being permanently lost.

III. ARGUMENT

A. Defendants' Widespread and Willful Spoliation of Evidence Highly Relevant to Synopsys' Case Warrants a Sanction of Default Judgment on Synopsys' DMCA Claims.

Defendants admit that they destroyed evidence, and thus there is no dispute that they are guilty of spoliation. *E.g.*, Ex. PP (Nisenbaum Decl.) ¶¶ 4-5 (Tsai used "CCleaner to wipe portions of [his] external drive," engaged in conversations about "wiping computers," and "instructed an unknown number of ASIC team member to destroy documents"); Ex. QQ (Ubiquiti & UNIL Answer) ¶ 121 (admitting "Tsai used … CCleaner," "Wang's computer contained virtual machines that appeared to contain deleted Synopsys files," "Huang ran CCleaner twice in March 2018," Lian deleted "files that had the word 'Synopsys' in them," Y.C. Yang "used AVG File Shredder [and] CCleaner," and C.C Yang "used CCleaner in March 2018"). The only real issue is what sanction is warranted in light of the extent and nature of the spoliation.

Courts have the inherent power to sanction spoliation. *Doe v. Cty. of San Mateo*, No. 3:15-cv-05496-WHO, 2017 WL 6731649, at *4 (N.D. Cal. Dec. 29, 2017) (Orrick, J.) (quoting *Chambers v. NASCO, Inc.*, 501 U.S. 32, 43 (1991)). In addition, Federal Rule of Civil Procedure 37(e) authorizes sanctions for a party's failure to take reasonable steps to preserve electronically stored information ("ESI") when the lost data cannot be replaced through other discovery. *Matthew Enter., Inc. v. Chrysler Grp. LLC*, No. 13-cv-4236-BLF, 2016 WL 2957133, at *3 (N.D. Cal. May 23, 2016). Under Rule 37(e)(2), when a party intentionally destroys evidence, the court may impose terminating sanctions, presume the destroyed evidence was unfavorable, or give the jury an adverse inference instruction. Spoliation need only be shown by a preponderance of the evidence. *Compass Bank v. Morris Cerullo World Evangelism*, 104 F. Supp. 3d 1040, 1053 (S.D. Cal. 2015). Synopsys seeks sanctions under both the Court's inherent powers and Rule 37(e)(2).

1. Defendants Failed to Preserve Evidence as Required by Law.

Defendants failed to preserve evidence in violation of Rule 37(e), which required them to "take reasonable steps to preserve" ESI. Defendants' complete lack of action after receiving the

May 10, 2016 ITCA Notice, their failure to preserve data on the AME Team's devices, and their decision not to prevent automatic deletions on their servers all violate Rule 37(e).

The duty to preserve begins as soon as litigation is reasonably anticipated or a potential claim is identified. *Rockman Co. (USA) v. Nong Shim Co.*, 229 F. Supp. 3d 1109, 1122 (N.D. Cal. 2017); *Apple Inc. v. Samsung Elecs. Co.*, 881 F. Supp. 2d 1132, 1136 (N.D. Cal. 2012). "As soon as a potential claim is identified, a litigant is under a duty to preserve evidence which it knows or reasonably should know is relevant to the action[.]" *Compass Bank*, 104 F. Supp. 3d at 1051. A litigant need not demand that an adverse party preserve evidence, though a formal request to preserve evidence has been found to trigger the duty. *Apple*, 881 F. Supp. 2d at 1136.

Defendants' duty to preserve arose here on May 10, 2016, when Synopsys' agent ITCA notified Defendants that they were infringing Synopsys' copyrights and threatened litigation. [redacted] Ex. S at 80. [redacted] *Id.* [redacted] *Id.*

The ITCA Notice put Defendants on notice that there was a potential claim against them for unlicensed use of copyrighted software. *See Keithley v. Home Store.com, Inc.*, No. C-03-04447 SI (EDL), 2008 WL 3833384, at *6 (N.D. Cal. 2008) (duty to preserve arose two years before suit after letter asserting infringement and indicating willingness to litigate); *Doe v. Norwalk Cmty. Coll.*, 248 F.R.D. 372, 377 (D. Conn. 2007) (duty to preserve arose via a demand letter indicating intent to sue). [redacted] Ex. KK (Nisenbaum email to Tsai). Yet Defendants took no action to preserve evidence after receiving the ITCA Notice, which allowed Tsai and other AME Team members to destroy highly relevant evidence, including log files, pirated software, counterfeit license keys, key generating software, and electronic communications.

Defendants also failed to preserve evidence even after suit was filed, as proven by the substantial spoliation that occurred after the Complaint was filed in February 2017 and even after Judge Beeler's 2018 order that AME Team devices outside the United States were discoverable. Forensics investigation revealed that from February 2017 through March 2018, Defendants systematically and deliberately wiped data and attempted to cover up their spoliation. Roffman Decl. ¶ 7; Ex. D at 9-11, 48-59. Defendants plainly had a duty to preserve evidence during this period and not only failed to do so, but intentionally destroyed evidence and covered their tracks.

Due to Defendants' failure to collect and preserve evidence in a timely manner and prevent destruction of evidence, critical evidence is now gone, and Synopsys cannot fully know what evidence existed or what it would have shown. This is sanctionable spoliation. *See, e.g.*, *Matthew Enter.*, 2016 WL 2957133, at *4-5 (failing to retain emails from previous email system); *Apple Inc. v. Samsung Elecs. Co.*, 888 F. Supp. 2d 976, 991-92 (N.D. Cal. 2012) (failure to stop automatic email deletion); *Herson v. City of Richmond*, No. C 09-02516 PJH (LB), 2011 WL 3516162, at *2-4 (N.D. Cal. Aug. 11, 2011) (installing new operating system that "effectively deleted all the files on the hard drive"); *Moore v. Gilead Scis., Inc.*, No. C 07-03850 SI, 2012 WL 669531, at *1 (N.D. Cal. Feb. 29, 2012) (using wiping software six times to erase data).

2. Defendants Intentionally Destroyed Evidence.

Defendants' destruction of ESI was pervasive and deliberate. Defendants deleted entire libraries of files, used wiping and "shredder" programs to permanently delete data, overwrote hard drives with large files, deleted chat data, and used commands to specifically search out and destroy Synopsys software and related command log history files. Had it not been destroyed, this evidence would have been at the heart of Synopsys' case, further proving the number, nature, circumstances, and place of the violations and corroborating Synopsys's call-home data. Defendants' rampant spoliation has deprived Synopsys of critical evidence.

This is precisely the sort of conduct that constitutes willful and intentional spoliation warranting terminating sanctions. In *Leon v. IDY Systems Corp.*, 464 F.3d 951 (9th Cir. 2006), an employer sought court approval to fire an employee, who claimed termination would be retaliatory and discrimination based on disability. Discovery revealed that the employee intentionally deleted “more than 2,200 files” on his work laptop, and, after the suit was filed, wiped “all [the] data in the hard drive’s unallocated space.” *Id.* at 956. The Ninth Circuit upheld a terminating sanction because the employee willfully deleted files “potentially relevant to the litigation.” *Id.* at 959. “[A]lthough it is impossible to identify which files and how they might have been used,” “any number of the 2,200 files could have been relevant” to whether there was a bona fide basis for retaliation and whether the employee had a disability. *Id.* at 960. Anything short of default risked benefiting the employee-spoliator and disadvantaging the employer. *Id.*

Likewise, terminating sanctions were warranted in *OmniGen Research v. Wang*, 321 F.R.D. 367, 372 (D. Or. 2017), when defendants “made their desktop computer unavailable,” “intentionally deleted thousands of documents,” “intentionally deleted and refused to produce relevant emails,” and “intentionally destroyed metadata.” The court found that at least some of deletions occurred during litigation after defendants were ordered to preserve and produce ESI. *Id.* at 373. In a case involving trade secret misappropriation, copyright infringement, unfair competition, intentional interference with economic relations, among others, the court held that defendants’ willful spoliation “deprived the Plaintiffs of evidence central to their case and undermined the Court’s ability to enter a judgment based on the evidence.” *Id.*; *see also Stanley Black & Decker, Inc. v. D&L Invs., LLC*, No. C 12-04516 SC (LB), 2014 WL 3738327, at *5, *9-11 (N.D. Cal. June 20, 2014) (Beeler, M.J.) (recommending case-terminating sanctions because Defendants “recycled” a laptop a day after the plaintiff asked defendants to begin producing information from it and refused to sit for a deposition or participate in the litigation).

These cases pale in comparison to our case, where the facts show that the spoliation was systematic, deliberate, calculated to avoid production in this case, and targeted at incriminating evidence. Under the circumstances, nothing short of terminating sanctions is appropriate.

3. The Evidence Defendants Destroyed Cannot be Restored or Replaced.

Rule 37(e) provides for sanctions when ESI is lost and “cannot be restored or replaced through additional discovery.” Because ESI “often exists in multiple locations, loss from one source may often be harmless when substitute information can be found elsewhere.” Fed. R. Civ.

P. 37(e) Adv. Comm. Notes to 2015 Amendment. The spoliators here made sure that the evidence would be gone, even if it existed in multiple locations. Nearly all relevant custodians deliberately deleted evidence on multiple computers, external hard drives, and servers. Defendants have not identified other locations where the deleted evidence might still reside, nor produced evidence to replace the destroyed files. On the contrary, Defendants contend they have no idea what was deleted. Ex. QQ (Ubiquiti & UNIL Answer) ¶ 98; Ex. LL at 98:10-101:9.

4. Defendants' Destruction of Evidence Has Prejudiced Synopsys.

Under Rule 37(e)(2), Synopsys is not required to show that the intentional destruction of evidence caused it prejudice.[10] Fed. R. Civ. P. 37(e)(2), Adv. Comm. Notes to 2015 Amendment. "This is because the finding of intent required by the subdivision can support not only an inference that the lost information was unfavorable to the party that intentionally destroyed it, but also an inference that the opposing party was prejudiced by the loss of information that would have favored its position." *Id.*; *accord OmniGen*, 321 F.R.D. at 371-72 ("A finding of intent, however, eliminates the requirement that the opposing party be prejudiced by the spoliation."). Similarly, under the Court's inherent powers, "because the relevance of destroyed documents cannot be clearly ascertained because the documents no longer exist, a party can hardly assert any presumption of irrelevance as to the destroyed documents." *Leon*, 464 F.3d at 959.

That said, Synopsys can easily show prejudice here. Many of the deleted files went to the heart of this case. According to Synopsys' forensic analysis, the deletions were often targeted at evidence of software that Synopsys alleges Defendants pirated, counterfeit keys, license key generation software, virtual machines used to carry out the piracy, and logs that would have provided detailed information about the nature, number, circumstances, and place of Defendants' violations. These include files on the devices of crucial AME Team members—notably, Tsai, Wang, and Lian—as well as critical data on UNIL's servers that was intentionally or automatically deleted, and unproduced and/or unpreserved devices and cloud storage facilities. *Id.* In a case about software piracy, the software itself, electronic communications, and usage logs are among the most important evidence a plaintiff can have, and that is what Defendants destroyed.

[10] Though prejudice is relevant in determining whether default should be imposed. *Infra* 22-23.

Moreover, there is data from between May 10, 2016 and the filing of the Complaint in February 2017 (when the call-home data was blocked) that one would have expected to find but are simply missing. These include chat data in the wake of the ITCA Notice, after Tsai told his team to take their discussions about Synopsys' software to an external chat program rather than email. Ex. KK. Under the circumstances, it is likely those chat communications directly concerned the piracy and the cover-up. *See Apple*, 881 F. Supp. 2d at 1149 (finding prejudice where, even though "the court will never know how much relevant material was lost," the time period suggested that the most relevant emails were deleted). Indeed, the limited number of chats that Synopsys was able to recover are seriously incriminating. Ex. P at 85 (lines 3723-3728) [redacted]

5. Defendants' Substantial, Coordinated, and Deliberate Spoliation of Key Evidence on a Massive Scale Requires Terminating Sanctions.

Rule 37(e)(2) permits a court to issue three types of sanctions for intentional spoliation: (1) a presumption that the lost evidence was unfavorable to the spoliating party, (2) an instruction to the jury that it may or must presume the information was unfavorable to the spoliating party, and (3) default judgment. Fed. R. Civ. P. 37(e)(2). Defendants' conduct here is so egregious, so willful, and so widespread that it requires default judgment on Synopsys' DMCA claims—all of which are directly impacted by Defendants' spoliation.

A default judgment for spoliation requires "a finding of willfulness, fault or bad faith." *OmniGen*, 321 F.R.D. at 371. All three exist here. The deliberate deletion, wiping, and shredding of inculpating files—often days or even minutes before imaging—demonstrates both Defendants' fault and bad faith. "A party's destruction of evidence qualifies as willful spoliation if the party has some notice that the documents were *potentially* relevant to the litigation before they were destroyed." *Leon*, 464 F.3d at 959. As detailed (at 8-13), Defendants destroyed the evidence they knew was the most relevant and the most incriminating: counterfeit keys, key generation software, virtual machines that carried out the piracy, and locally stored logs that documented it all. Defendants' fault, bad faith, and willfulness is indisputable.

Before imposing default judgment, courts consider five factors: (1) the public's interest in expeditious resolution of litigation, (2) the court's need to manage its docket, (3) the risk of prejudice to the party seeking sanctions, (4) the public policy favoring disposition of cases on their merits, and (5) the availability of less drastic sanctions. *Id.* at 958. Because "the first two of these factors favor the imposition of sanctions in most cases" and "the fourth cuts against a default or dismissal sanction" in most cases, "the key factors are prejudice and availability of lesser sanctions." *Wanderer v. Johnston*, 910 F.2d 652, 656 (9th Cir. 1990). These factors weigh overwhelmingly in favor of default judgment.

Judicial Interests. The first two factors—the public's interest in expeditious resolution of litigation and the Court's need to manage its docket—either "always" or "almost always" favor default judgment in circumstances like this. *CFPB v. Morgan Drexen, Inc.*, 101 F. Supp. 3d 856, 872-73 (C.D. Cal. 2015) (granting terminating sanctions). This case is no different: Defendants' actions have undermined the judicial process and impeded Synopsys' case.

Prejudice. A party suffers prejudice sufficient to warrant a default judgment when spoliation threatens its "ability to go to trial" or "interfere[s] with the rightful decision of the case." *Leon*, 464 F.3d at 959. Forcing a party to go to trial on "incomplete" evidence is prejudicial. *Stanley Black & Decker*, 2014 WL 3738327, at *10 (citing *Anheuser-Busch, Inc. v. Natural Bev. Distribs.*, 69 F.3d 337, 354 (9th Cir. 1995)). The "failure to produce documents as ordered is by itself prejudice enough to authorize terminating sanctions." *Id.*

As discussed above, Defendants' spoliation has caused significant prejudice to Synopsys. Although Synopsys believes it can still prove its claims, it should not have to do so with one arm tied behind its back while the judge and jury are limited by an incomplete record. To name just a few, this includes (1) missing data corroborating Synopsys' call-home data, (2) evidence of even more extensive piracy of Synopsys' software than is currently of record because Defendants blocked call-home data after May 2016, (3) evidence Synopsys would have used to rebut Defendants' arguments that its circumventions and traffickings are extraterritorial and not compensable, (4) further discussions among the conspirators, and (5) other evidence showing a coordinated effort to engage in a pattern of unlawful acts and to cover up those crimes. Defendants' conduct unquestionably "threaten[s] to distort the resolution" of the case. *Leon*, 464 F.3d at 960.

Public Policy. Where, as here, a party's conduct has already compromised a full and fair determination on the merits, the public policy favoring disposition of cases on the merits "weighs only slightly against terminating sanctions." *Morgan Drexen*, 101 F. Supp. 3d at 874. In a case like this, this factor is therefore "insufficient to outweigh the other four factors." *Id.*

Lesser Sanctions. "The Court may dismiss the case based on spoliation of evidence where (1) less drastic sanctions would be inappropriate, (2) the Court implemented alternative sanctions before ordering dismissal, and (3) the Court warned the party of dismissal before ordering dismissal." *Id.* (citations omitted). The second and third factors are often inapplicable when, as here, a party has destroyed evidence before a court can compel discovery, order other lesser sanctions, or issue warnings. *Id.* at 875; *see also Leon*, 464 F.3d at 960. Here, in addition to destroying evidence before and during this litigation that they were obligated to preserve, Defendants continued to spoliate evidence after Judge Beeler held that their devices in Taiwan were discoverable, *supra* 13, and after the Court explicitly warned the parties about preservation. Judge Beeler's standing order, served on the parties in December 2017, warns them that they "must take the steps needed to preserve information relevant to the issues in this action, including suspending any … destruction programs for electronically-maintained material[]." Ex. XX at 2.

As to the first factor, there is no less drastic sanction commensurate with Defendants' egregious conduct that does not end up benefiting Defendants for their spoliation. A lesser sanction "is not appropriate if it would reward a defendant for its misconduct." *Morgan Drexen*, 101 F. Supp. 3d at 874. Anything short of a default benefits Defendants by affording them an opportunity to exploit the evidentiary holes in the record that their spoliation created. Synopsys has a right under the DMCA to statutory damages on a per-violation basis. *See* 17 U.S.C.

§ 1203(c)(3)(A). Defendants' primary response to Synopsys' DMCA claims is to contest the number of circumventions and traffickings. Absent default judgment that Defendants violated the DMCA 38,393 times, Defendants can abuse the limits of the knowable data, available logs, and preserved chats to diminish the number of violations and dispute the reliability of the call-home data, which can no longer be fully corroborated because of Defendants' spoliation. This is true with regard to the number of circumventions documented by the call-home data and the trafficking claims, where evidence of manufacture, provision, and trafficking of circumvention technology, devices, and services has been destroyed.

That said, a preclusion order that Defendants cannot contest the number of circumventions and incidents of trafficking still allows Defendants to benefit by arguing that the circumventions and traffickings are not "violations" of the DMCA because they occurred abroad and are extraterritorial. Here again, Defendants intentionally spoliated the electronic footprints and logs that Synopsys would have used to establish the physical and digital location of persons, computers, networks, and servers engaged in the piracy.[11] Having deliberately destroyed that evidence, Defendants should not now be allowed to benefit from the absence of that evidence to support their position that the acts occurred outside the United States.[12]

At the same time, it is important to note that Synopsys is not asking for the most severe sanction to which it is entitled. Given the willful and widespread spoliation, Synopsys would be

[11] For example, Defendants' extraterritoriality argument is predicated on the assertion that "egress IP" information in Synopsys' call-home data establishes the location of the relevant misconduct. But, the egress IP is the IP address from which the call-home signals exit Defendants' corporate network; it says nothing about the actual or digital location of the person or computer up stream that executed the piracy, just as it says nothing about the location of other occurrences in the illegal chain of events (*i.e.*, unauthorized copying, counterfeiting, etc.). As Defendants concede, when users in the United States remotely accessed software on Taiwan servers, the call-home signals sent out made it appear as if the users were physically present at the server in Taiwan. Ex. M ¶ 30; Ex. YY ¶¶ 10-12. [redacted] Roffman Decl. ¶¶ 13-28. This evidence also would have helped show the extensive relationship of Defendants' acts to the United States, such as illegally downloading, copying, and trafficking software and counterfeit key in the United States.

[12] An instruction to the jury is insufficient because it still leaves Synopsys "helpless to rebut any material that [the spoliating party] might use to overcome the presumption." *Leon*, 464 F.3d at 960. Instructing the jury to presume that Defendants destroyed evidence unfavorable to them does not quantify how many times Defendants unlawfully circumvented Synopsys' security software or how many times Defendants trafficked in circumvention technology or services.

well within its rights to seek default on all claims. Synopsys also would be within its rights to ask for default not just as to the 38,393 violations in the call-home data before Defendants blocked the signals, but all 54,827 violations Synopsys believes were committed. *Supra* 5 n.5. Synopsys has not done so. Synopsys has limited its sanctions request to only its DMCA claims and to only those violations reported in the call-home data, for which Synopsys has been deprived of evidence of the precise nature, circumstances, and place of Defendants' violations.

B. In the Alternative, Synopsys Requests Issue Preclusion Orders, Adverse Inference Instructions, and All Other Appropriate Relief.

If the Court declines to enter default judgment, it should issue all, or at the very least some combination of, the following: (1) an order precluding Defendants from contesting the number of circumventions, as shown in the call-home data, (2) an order precluding Defendants from contesting that the circumventions and traffickings are compensable violations of the DMCA, and are not extraterritorial, (3) an instruction that the jury shall infer that the destroyed evidence was incriminating in that it tended to prove Defendants' violations of the DMCA, including, but not limited to, that Defendants' violations "occurred in the United States," and (4) any other relief this Court deems appropriate. In the event alternative relief is ordered, Synopsys should have the right to prove the extent of spoliation to the jury. Although Synopsys seeks these alternative sanctions in the absence of a terminating sanction, for the reasons just discussed, such sanctions cannot fully alleviate the harm to Synopsys' case caused by Defendants' destruction of evidence.

IV. CONCLUSION

This Court should grant Synopsys default judgment that Defendants are liable for 38,393 violations of the DMCA, 17 U.S.C. §§ 1201(a)(1), (a)(2), and (b), and that Synopsys is entitled to an award of damages for those violations in an amount to be determined at trial. In the alternative, the Court should issue orders of preclusion, instruct the jury to draw adverse inferences, and order any and all other relief the Court deems appropriate.

Dated: October 3, 2018

DENISE M. MINGRONE
CLAUDIA WILSON FROST
ROBERT L. URIARTE
ORRICK, HERRINGTON & SUTCLIFFE LLP

By: */s/ Denise M. Mingrone*
DENISE M. MINGRONE

Attorneys for Plaintiff
SYNOPSYS, INC.